

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION**

MICHELLE RODGERS , individually and on behalf of herself and all others similarly situated, Plaintiff, v. NEC NETWORKS LLC dba CAPTURERX , Defendant.	Case No. 5:21-cv-692 <u>CLASS ACTION COMPLAINT</u> JURY TRIAL DEMANDED
---	--

Plaintiff Michelle Rodgers (“Plaintiff” or “Plaintiff Rodgers”), individually and on behalf of all other similarly situated, by and through her attorneys, upon personal knowledge as to themselves and their own acts and experiences, and upon information and belief as to all other matters, including their counsel’s investigation, alleges as follows. Plaintiff believes additional evidentiary support exists for their allegations, given an opportunity for discovery.

NATURE OF THE ACTION

1. Plaintiff, individually and on behalf of all others similarly situated, brings this Class Action Complaint (“Complaint”) against Defendant NEC Networks LLC dba CaptureRx (“Defendant” or “CaptureRx”) based on Defendant’s failure to properly safeguard its customers’ current and former patients’ (“Class Members”) personally identifiable information (“PII”), including Class Members’ full names, dates of birth and addresses. Defendant also failed to properly safeguard Class Members’ protected health information (“PHI”), including prescription medication data and medical record numbers.

2. CaptureRx is a large provider of Section 340B administrative services to healthcare providers. CaptureRx processes 340B Drug Pricing Program prescription claims using its specifically developed computer software.

3. On or about February 6, 2021, as a result of CaptureRx's lax security and monitoring protocols, criminals gained unauthorized access to CaptureRx system and acquired sensitive records belonging to CaptureRx's clients (the "Data Breach"). Currently, it is believed that the sensitive PII and PHI of nearly two million individuals was exposed in the Data Breach.

4. As a result of these lax security and monitoring protocols, CaptureRx did not detect this massive Data Breach until February 19, 2021.

5. Inexplicably, CaptureRx did not begin notifying the individual victims of the breach until May of 2021. For example, Plaintiff received letters about the Data Breach dated May 18, 2021.

6. CaptureRx did not adequately safeguard Plaintiff's data, and now she and apparently millions of other patients are the victims of a significant data breach that will negatively affect them for years.

7. CaptureRx is responsible for allowing this Data Breach through its failure to implement and maintain reasonable safeguards and failure to comply with industry-standard data security practices as well as federal and state laws and regulations governing data security, including security of PHI.

8. Despite its role in managing so much sensitive and personal PII and PHI, during the duration of the data breach, CaptureRx failed to recognize and detect unauthorized third parties accessing its system, and failed to recognize the substantial amounts of data that had been compromised. This was, in part, because of, but also part and parcel with, CaptureRx's failure to

take the appropriate steps to investigate the numerous red flags, each of which individually should have told CaptureRx that its systems were not secure.

9. During the duration of the Data Breach, CaptureRx failed to, among other things, detect that ill-intentioned criminals had accessed its computer data and storage systems, notice the massive amounts of data that were compromised, and take any steps to investigate the red flags that should have warned CaptureRx that its systems were not secure. Had CaptureRx properly monitored its information technology infrastructure, it would have discovered the invasion sooner.

10. CaptureRx had numerous statutory, regulatory, and common law obligations to Plaintiff and the Class Members to keep their PII, including PHI, confidential, safe, secure, and protected from unauthorized disclosure or access, specifically including the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Plaintiff and those similarly situated rely upon CaptureRx to maintain the security and privacy of the PII and PHI entrusted to it; when providing their PII and or PHI to CaptureRx’s clients, they reasonably expected and understood that the vendors of CaptureRx’s clients would comply with its obligations to keep the information secure and safe from unauthorized access.

11. In this day and age of regular and consistent data security attacks and data breaches, particularly in the healthcare industry, CaptureRx’s Data Breach is particularly egregious.

12. By obtaining, collecting, using, and deriving benefit from Plaintiff’s and Class Members’ PII and PHI, CaptureRx assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff’s and Class Members’ PII and PHI from disclosure.

13. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI.

14. Plaintiff and Class Members relied on CaptureRx to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

15. As a result of CaptureRx's failures to protect the PII and PHI of Plaintiff and Class Members, their PII and PHI were accessed by malicious cyber criminals. Therefore, Plaintiff and the Class Members are at a significant present and future risk of identity theft, financial fraud, and/or other identity theft or fraud, imminently and for years to come. Common sense dictates that this was the sole reason the unauthorized third parties breached CaptureRx's system and acquired its sensitive patient records.

16. Just as their PII and PHI was stolen because of its inherent value in the black market, now the inherent value of Plaintiff and the Class Members' PII and PHI in the legitimate market is significantly and materially decreased. To make matters worse, the injuries described were exacerbated by CaptureRx's failure to timely inform and notify Plaintiff and the Class Members of the data breach and their injuries. Furthermore, by failing to provide adequate notice, CaptureRx intentionally prevented Plaintiff and prospective Class Members from protecting themselves from the potential damages arising out of the data breach.

17. Plaintiff and members of the proposed Class have suffered actual and imminent injuries as a direct result of the Data Breach. The injuries suffered by Plaintiff and the proposed Class as a direct result of the Data Breach include: (a) theft of their personal data; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the consequences of the Data Breach and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach; (d) the actual and/or imminent injury arising from

actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (e) damages to and diminution in value of their personal data entrusted to CaptureRx and with the mutual understanding that CaptureRx would safeguard Plaintiff's and Class Members' personal data against theft and not allow access and misuse of their personal data by others; (f) the reasonable value of the PII entrusted to CaptureRx; and (g) the continued risk to their personal data, which remains in the possession of CaptureRx and which is subject to further breaches so long as CaptureRx fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' personal data in its possession.

18. Plaintiff seeks to remedy these harms, and prevent their future occurrence, on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach.

19. Accordingly, Plaintiff, on behalf of herself and other members of the Class, assert claims for negligence, negligence *per se*, and declaratory judgment. Plaintiff seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

20. Plaintiff Rodgers a resident of Arkansas.

21. Plaintiff Rodgers received health services from ARcare, which entrusted Plaintiff Rodgers's PII and PHI to CaptureRx.

22. Plaintiff Rodgers received two letters from CaptureRx concerning the Data Breach, one of which was addressed to her personally, and another addressed to her as guardian of A.H., her daughter. Both letters were dated May 18, 2021. The letters stated that the full names, dates of birth, and prescription information for Plaintiff Rodgers and A.H. were compromised in the Data

Breach. The letters further stated that, “on or around March 19, 2021, CaptureRx confirmed” their PII and PHI was included in the Data Breach. Yet, Plaintiff Rodgers was not notified of the Data Breach until receiving the letters from CaptureRx in mid to late May 2021.

23. Since learning of the Data Breach, Plaintiff Rodgers has suffered emotional anguish and distress, including but not limited to worrying about her personal, private PII and PHI being in the hands of authorized individuals. She also has suffered mental anguish because her daughter, A.H.’s, PII and PHI are in the hands of unauthorized individuals.

24. As a result of the breach, Plaintiff Rodgers has spent substantial time weekly reviewing her personal, financial, and credit account. She’s received notifications that her personal information has been comprised since the breach occurred, including but not limited to receiving increased spam emails, phone calls claiming to be government agencies, and someone accessing her Facebook account to start an advertisement campaign. As a result, Facebook keeps attempting to charge her for the Facebook advertisement.

25. CaptureRx is a limited liability company organized in the State of Texas with its principal place of business in San Antonio, Texas.

JURISDICTION & VENUE

26. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative Class Members and the amount in controversy exceeds \$5,000,000, exclusive of interest and costs. Plaintiff (and many members of the Class) and Defendant are citizens of different states.

27. This Court has general personal jurisdiction over CaptureRx because CaptureRx’s principal place of business is in San Antonio, Texas.

28. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and

1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and CaptureRx conducts substantial business in this District.

FACTUAL ALLEGATIONS

29. CaptureRx is a large provider of Section 340B administrative services to healthcare providers. CaptureRx processes 340B Drug Pricing Program prescription claims using its specifically developed computer software.¹

30. Section 340B of the Public Health Services Act requires pharmaceutical manufacturers participating in Medicaid to sell outpatient drugs at discounted prices to health care organizations that care for many uninsured and low-income patients. These organizations include community health centers, children's hospitals, hemophilia treatment centers, critical access hospitals (CAHs), sole community hospitals (SCHs), rural referral centers (RRCs), and public and nonprofit disproportionate share hospitals (DSH) that serve low-income and indigent populations.²

31. As a condition of providing administrative services to its health care provider clients, CaptureRx requires that its clients entrust it with the highly sensitive PII and PHI of their patients.

32. CaptureRx publicly represents that its "customers can have a high level of peace of mind knowing that we secure the data that is processed and transmitted through our system."³ Contrary to this representation, CaptureRx did not secure the data processed and transmitted through its system.

The Data Breach

33. On or about February 6, 2021, criminals gained unauthorized access to CaptureRx

¹ <https://www.hhhn.org/news/CaptureRx-data-breach/> (last visited July 20, 2021).

² <https://www.aha.org/fact-sheets/2020-01-28-fact-sheet-340b-drug-pricing-program> (last visited May 25, 2021).

³ <https://www.CaptureRx.com/soc2-compliance/> (last visited July 20, 2021).

system and acquired sensitive records belonging to CaptureRx's clients.⁴ These records contained the sensitive PII and PHI of CaptureRx's clients' patients.

34. The unauthorized third parties were able to gain access to CaptureRx's system as a result of CaptureRx's failure to take necessary and required minimal steps to secure Plaintiff Rodgers's, A.H.'s, and the Class Members' PII and PHI.

35. CaptureRx did not detect the Data Breach until February 19, 2021.⁵

36. CaptureRx clients with patient data exposed in the breach are believed to include, but not be limited to: Faxton St. Luke's Healthcare, an affiliate of Mohawk Valley Health System; Jordan Valley Community Health Center; Hudson Headwaters Health Network; Gifford Health Care; Thrifty Drug Stores; Brownsville Community Health Center; UPMC Cole; Our Lady of Lourdes Memorial Hospital; Ascension St. Joseph Hospital; Ascension Standish Hospital; Hidalgo Medical Services; Adirondack Health; Kaleida Health; Bayhealth; and Walmart.⁶

37. As of the date of filing of this Complaint, it is believed the Data Breach exposed the sensitive PII and PHI of 1,919,938 individuals.⁷

38. CaptureRx did not begin notifying the individual victims of the breach until May of 2021. For example, Plaintiff Rodgers and A.H. received letters dated May 18, 2021 from CaptureRx notifying them of the Data Breach.

39. Notably, the notification letter received by Plaintiff Rodgers stated, in part:

What Happened? CaptureRx recently became aware of unusual activity involving certain of its electronic files. Following this, CaptureRx immediately began an investigation into

⁴ <https://www.prnewswire.com/news-releases/CaptureRx--notice-of-data-incident-301284905.html> (last visited May 25, 2021).

⁵ <https://www.prnewswire.com/news-releases/CaptureRx--notice-of-data-incident-301284905.html> (last visited July 20, 2021).

⁶ <https://www.hipaajournal.com/CaptureRx-ransomware-attack-affects-multiple-healthcare-provider-clients/> (last visited July 20, 2021).

⁷ <https://www.hipaajournal.com/CaptureRx-ransomware-attack-affects-multiple-healthcare-provider-clients/> (last visited July 20, 2021).

this activity and worked quickly to assess the security of its systems. On February 19, 2021, the investigation determined that certain files were accessed and acquired on February 6, 2021 without authorization.

CaptureRx immediately began a thorough review of the full contents of the files to determine whether sensitive information was present at the time of the incident. On or around March 19, 2021, CaptureRx confirmed that some of your information was present in the relevant files. CaptureRx began the process of Notifying ARcare on or around March 30, 2021 of this incident.

What Information Was Involved? The investigation determined that, at the time of the incident, the relevant files contained your first name, last name, date of birth, and prescription information. We are providing you this notice to ensure you are aware of this incident.

What Is CaptureRx Doing? Data privacy and security are among CaptureRx's highest priorities, and there are extensive measures in place to protect information in CaptureRx's care. Upon learning of this incident, CaptureRx moved quickly to investigate and respond. This investigation and response included confirming the security of CaptureRx's systems, reviewing the contents of the relevant files for sensitive information, and notifying business partners associated with that sensitive information. As part of CaptureRx's ongoing commitment to the security of information, all policies and procedures are being reviewed and enhanced and additional workforce training is being conducted to reduce the likelihood of a similar future event.

40. To date, CaptureRx has not offered to provide Plaintiff, A.H. or (upon information and belief) the Class Members with any compensation or remedy related to the exposure of their sensitive PII and PHI.

CaptureRx Acknowledges the Harm this Data Breach Has and Will Cause the Victims

41. It is common sense that the criminals that breached CaptureRx's systems and acquired the victims' PII and PHI did so for the purpose of using that data to commit fraud, theft, and other crimes, or for the purpose of the selling or providing the PII and PHI to other individuals intending to commit fraud, theft, and other crimes. Given that this is the reason such PII and PHI is sought by criminals, it is similarly common sense that Plaintiff Rodgers and the Class Members have already suffered injury and face a substantial risk for imminent future injury.

42. CaptureRx acknowledges the risk faced by victims of the breach. For example, its

notification letters state, in part: “We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors.”

43. Furthermore, the notification letters sent to Plaintiff Rodgers and Class Members include a document titled “STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION.” In addition to the information discussed above, this document informs victims that they may wish to place initial or extended fraud alerts on credit files or obtain a credit freeze by contacting each of the three major credit reporting bureaus.

44. CaptureRx acknowledges that victims following the advice to obtain a credit freeze will be further inconvenienced and harmed as a result of taking these reasonable steps to prevent future harm. Specifically, it states that “you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.”

CaptureRx Knew it Was and Continues to be a Prime Target for Cyberattacks.

45. CaptureRx is fully aware of how sensitive the PII and PHI it stores and maintains is. It is also aware of how much PII and PHI it collects, uses, and maintains from each Plaintiff or Class member.

46. CaptureRx knew or should have known that it was an ideal target for hackers and those with nefarious purposes related to sensitive personal and health data. It processed and saved multiple types and many levels of PII and PHI through its computer data and storage systems.

47. By requiring the production of, collecting, obtaining, using, and deriving benefits

from Plaintiff's, and the Class Members', PII and PHI, CaptureRx assumed certain legal and equitable duties and knew or should have known that it was responsible for the diligent protection of the PII and PHI it collected and stored.

48. Realizing its duty with respect to PII and PHI, CaptureRx's website Privacy Policy⁸ states:

Your privacy is important to CaptureRx, and we are committed to adhering to federal and state privacy laws and industry guidelines for using personal information collected from the Website in order to protect you and your identity.

49. Similarly, the notification letters acknowledge the importance of data security and its duty to the Class Members, stating that "[d]ata privacy and security are among CaptureRx's highest priorities...."

50. As a large and highly successful company, CaptureRx had the resources to invest in the necessary data security and protection measures. Yet, CaptureRx failed to undertake adequate analyses and testing of its own systems, adequate personnel training, and other data security measures to avoid the failures that resulted in the Data Breach.

51. The seriousness with which CaptureRx should have taken its data security is shown by the number of data breaches perpetrated in the healthcare and retail industries in the last few years.

52. Over 41 million patient records were breached in 2019, with a single hacking incident affecting close to 21 million records.⁹ Healthcare breaches in 2019 almost tripled those the healthcare industry experienced in 2018, when 15 million patient records were affected by data

⁸ <https://CaptureRx.com/en-us/online-privacy-policy> (last visited July 20, 2021).

⁹ Heather Landi, *Number of patient records breached nearly triples in 2019*, Fierce Healthcare (Feb. 20, 2020), <https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=Over%2041%20million%20patient%20records,close%20to%2021%20million%20records>. (last visited July 20, 2021).

breach incidents, according to a report from Protenus and DataBreaches.net.¹⁰

53. Protenus, a healthcare compliance analytics firm, analyzed data breach incidents disclosed to the U.S. Department of Health and Human Services or the media during 2019, finding that there has been an alarming increase in the number of data breaches of patient privacy since 2016, when there were 450 security incidents involving patient data.¹¹ In 2019 that number jumped to 572 incidents, which is likely an underestimate, as two of the incidents for which there were no data affected 500 dental practices and clinics and could affect significant volumes of patient records. There continues to be at least one health data breach per day.¹²

54. One recent report found that in 2020, healthcare was one of the industries most affected by tracked ransomware incidents.¹³

The PII and PHI at Issue Here is Particularly Valuable to Hackers

55. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers, but credit and debit cards can be cancelled quickly mitigating the hackers' ability to cause further harm.

56. Instead, PHI and types of PII that cannot be changed (such as dates of birth) are the most valuable to hackers.¹⁴ Indeed, according to a report by the Federal Bureau of Investigation's ("FBI") Cyber Division, healthcare records can be sold by criminals for 50 times the price of stolen Social Security numbers or credit card numbers.¹⁵ A file containing private health insurance

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

¹³ <https://www.healthcareitnews.com/news/healthcare-hackers-demanded-average-ransom-46m-last-year-says-bakerhostetler> (last visited May 25, 2021).

¹⁴ <https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/> (last visited July 20, 2021).

¹⁵ Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014) available at <https://publicintelligence.net/fbi-health-care-cyber-intrusions/> (last visited July 20, 2021).

information can be bought for between \$1,200 and \$1,300 each on the black market.¹⁶

57. Similarly, the most recent edition of the annual Baker Hostetler Data Security Incident Response Report found that in 2020, hackers in ransomware attacks made an average initial ransomware demand of \$4,583,090 after obtaining PHI. In 2020, final payouts to hackers committing ransomware attacks involving PHI averaged \$910,335.¹⁷

58. Companies recognize that PII and PHI are valuable assets. Indeed, PII and PHI are valuable commodities. A “cyber black-market” exists in which criminals openly post stolen credit PII and PHI on a number of Internet websites. Plaintiff’s and Class Members’ personal data that was stolen has a high value on both legitimate and black markets.

59. Some companies recognize personal information, especially health information, as a close equivalent to personal property. Software has been created by companies to value a person’s identity on the black market. The commoditization of this information is thus felt by consumers as theft of personal property in addition to an invasion of privacy. Compromised health information can lead to falsified information in medical records and fraud that can persist for years as it “is also more difficult to detect, taking twice as long as normal identity theft.”¹⁸

60. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer’s personal information as follows:

The use of third-party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here

¹⁶ Elizabeth Clarke, *Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents* (July 15, 2013), available at <https://www.secureworks.com/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents> (last visited April 30, 2021).

¹⁷ <https://www.healthcareitnews.com/news/healthcare-hackers-demanded-average-ransom-46m-last-year-says-bakerhostetler> (last visited July 20, 2021).

¹⁸ See FBI CYBER DIVISION, (U) HEALTH CARE SYSTEMS AND MEDICAL DEVICES AT RISK FOR INCREASED CYBER INTRUSIONS FOR FINANCIAL GAIN 2 (2014), available at <https://publicintelligence.net/fbi-health-care-cyber-intrusions/> (FBI, April 8, 2014) (last visited July 20, 2021).

some time ago that it's something on the order of the life blood, the free flow of information.¹⁹

61. Consumers rightfully place a high value not only on their PII and PHI, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between \$11.33 and \$16.58 per website. The study also determined that “[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US\$30.49 – 44.62.”²⁰ This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII and PHI to bad actors—would be exponentially higher today.

62. According to the Federal Trade Commission (“FTC”), identity theft wreaks havoc on consumers’ finances, credit history, and reputation and can take time, money, and patience to resolve.²¹ Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.²²

¹⁹ FEDERAL TRADE COMMISSION, *The Information Marketplace: Merging and Exchanging Consumer Data*, transcript available at <http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data> (last visited July 20, 2021).

²⁰ Hann, Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Oct. 2002, available at <https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf> (last visited July 20, 2021).

²¹ See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), <http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf> (last visited July 20, 2021).

²² *Id.* The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 16 CFR § 603.2. The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” *Id.*

63. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims cannot be understated.²³ “A 2016 Identity Theft Resource Center survey of identity theft victims sheds light on the prevalence of this emotional suffering caused by identity theft: 74 percent of respondents reported feeling stressed, 69 percent reported feelings of fear related to personal financial safety, 60 percent reported anxiety, 42 percent reported fearing for the financial security of family members, and 8 percent reported feeling suicidal.”²⁴

64. The physical, emotional, and social toll suffered by victims of this Data Breach are even more profound because the Data Breach included prescription medication data. This means victims must deal with the stress, anxiety, and embarrassment that accompanies the very real possibility of friends, family, employers, and colleagues learning about sensitive medical conditions and diseases, such as sexually transmitted diseases, disabilities, and terminal illnesses.

65. More recently, the FTC has released its updated publication on protecting PII for businesses, which include instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

66. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect customers’ PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. § 45. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver’s license or identification card in the victim’s name but with another’s picture, and/or using the victim’s information to obtain a fraudulent refund. The United States

²³ *Id.*

²⁴ *Id.*

government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

67. Because the information CaptureRx allowed to be compromised and taken is of such a durable and permanent quality, the harms to Plaintiff and the Class will continue to grow, and Plaintiff and the Class will continue to be at substantial risk for further imminent and future harm.

CaptureRx's Post-Breach Activity was (and Remains) Inadequate

68. Immediate notice of a security breach is essential to protect people such as Plaintiff and the Class Members. CaptureRx failed to provide such immediate notice, in fact taking more than three months to disclose to victims that there had been a breach, thus further exacerbating the damages sustained by Plaintiff and the Class resulting from the breach.

69. Although CaptureRx purportedly “moved quickly” to notify its “business partners,” CaptureRx did not display the same sense of urgency in notifying the actual victims of the Data Breach, such as Plaintiff Rodgers. For example, taking the contents of the notification letters at face value, CaptureRx determined on February 19, 2021 that the Data Breach had occurred, and it specifically determined Plaintiff Rodgers’s and A.H.’s PII and PHI were included in the Data Breach on March 19, 2021. Yet, it did not attempt to notify Plaintiff Rodgers of the Data Breach until on or about May 18, 2021.

70. Such failure to protect Plaintiff’s and the Class Members’ PII and PHI, and timely notify of the breach, has significant ramifications. The information stolen allows criminals to commit theft, identity theft, and other types of fraud. Moreover, because all the data points stolen are persistent—for example, names, dates of birth, and prescription medication data—as opposed to transitory, criminals who purchase the PII and PHI belonging to Plaintiff and the Class Members

do not need to use the information to commit fraud immediately. The PII and PHI can be used or sold for use years later.

71. Plaintiff and the Class Members are at constant risk of imminent and future fraud, misuse of their PII and PHI, and identity theft for many years in the future as a result of the CaptureRx's actions and the data breach. The theft of PHI is particularly impactful, as many banks or credit card providers have substantial fraud detection systems with quick freeze or cancellation programs in place, whereas the breadth and usability of PHI allows criminals to get away with misuse for years before healthcare-related fraud is spotted.

72. Plaintiff Rodgers and the Class Members have suffered real and tangible loss, including but not limited to the loss in the inherent value of their PII and PHI, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries realized as a result of discovery in this case, but hitherto kept deliberately hidden by CaptureRx.

73. Despite CaptureRx's egregious failure to protect Plaintiff Rodgers's PII and PHI, it did not offer to provide them with any compensation or remedy, such as free credit monitoring or identity protection services. Upon information and belief, CaptureRx similarly did not offer to provide any compensation or remedy to the other victims of the Data Breach (i.e., Class Members).

CLASS ACTION ALLEGATIONS

74. Pursuant to the provisions of Rules 23(a), 23(b)(1), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure, Plaintiff bring this class action on behalf of herself and a nationwide class defined as:

All persons who reside in the United States whose personal data was compromised as a result of the Data Breach discovered by CaptureRx on or about February 19, 2021 (the "Class").

75. Excluded from the Class are Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

76. Plaintiff reserves the right to modify and/or amend the Class definition, including but not limited to creating additional subclasses, as necessary.

77. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

78. All members of the proposed Class are readily ascertainable in that CaptureRx has access to addresses and other contact information for all members of the Class, which can be used for providing notice to Class Members.

79. **Numerosity.** The Class is so numerous that joinder of all members is impracticable. The Class includes millions of individuals whose personal data was compromised by the Data Breach.

80. **Commonality.** There are numerous questions of law and fact common to Plaintiff and the Class, including the following:

- whether CaptureRx engaged in the wrongful conduct alleged in this Complaint;
- whether CaptureRx's conduct was unlawful;
- whether CaptureRx failed to implement and maintain reasonable systems and security procedures and practices to protect customers' personal data;
- whether CaptureRx unreasonably delayed in notifying affected customers of the

Data Breach;

- whether CaptureRx owed a duty to Plaintiff and members of the Class to adequately protect their personal data and to provide timely and accurate notice of the CaptureRx Data Breach to Plaintiff and members of the Class;
- whether CaptureRx breached its duties to protect the personal data of Plaintiff and members of the Class by failing to provide adequate data security and failing to provide timely and adequate notice of the CaptureRx Data Breach to Plaintiff and the Class;
- whether CaptureRx's conduct was negligent;
- whether CaptureRx knew or should have known that its computer systems were vulnerable to attack;
- whether CaptureRx's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach of its systems, resulting in the loss of Class Members' personal data;
- whether CaptureRx wrongfully or unlawfully failed to inform Plaintiff and members of the Class that it did not maintain computers and security practices adequate to reasonably safeguard customers' personal data;
- whether CaptureRx should have notified the public, Plaintiff, and Class Members immediately after it learned of the Data Breach;
- whether Plaintiff and members of the Class suffered injury, including ascertainable losses, as a result of CaptureRx's conduct (or failure to act);
- whether Plaintiff and members of the Class are entitled to recover damages; and
- whether Plaintiff and Class Members are entitled to declaratory relief and equitable

relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

81. **Typicality.** Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class Members, had their personal data compromised, breached and stolen in the CaptureRx Data Breach. Plaintiff and all Class Members were injured through the uniform misconduct of CaptureRx described in this Complaint and assert the same claims for relief.

82. **Adequacy.** Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff have retained counsel who are experienced in Class action and complex litigation. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other members of the class.

83. **Predominance.** The questions of law and fact common to Class Members predominate over any questions which may affect only individual members.

84. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, CaptureRx's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been harmed by CaptureRx's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to CaptureRx's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the

prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for CaptureRx. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing CaptureRx to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by the members of the Class would create risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

85. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

86. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because CaptureRx has acted and failed and refused to act in a manner that generally applies to all Class Members' PII and PHI in a manner, so final injunctive relief is appropriate with regard to the Class as a whole.

COUNT I **Negligence**

87. Plaintiff incorporates all other allegations included in paragraph 1 through 86 of this Complaint as of fully restate herein.

88. Plaintiff and Class Members were required to submit non-public PII and PHI to

obtain medical service benefits from CaptureRx's clients. CaptureRx required that its clients provide CaptureRx with this PII and PHI in order to receive CaptureRx's services.

89. By collecting, storing, and using Plaintiff's and Class Members' PII and PHI, CaptureRx owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive PII and PHI it received from being compromised, lost, stolen, accessed and misused by unauthorized persons.

90. CaptureRx was required to prevent foreseeable harm to Plaintiff and the Class Members, and therefore had a duty to take reasonable steps to safeguard sensitive PII and PHI from unauthorized release or theft. More specifically, this duty included: (1) designing, maintaining, and testing CaptureRx's data security systems and data storage architecture to ensure Plaintiff's and Class Members' PII and PHI were adequately secured and protected; (2) implementing processes that would detect an unauthorized breach of CaptureRx's security systems and data storage architecture in timely and adequate manner; (3) timely acting on all warnings and alerts, including public information, regarding CaptureRx's security vulnerabilities and potential compromise of the PII and PHI of Plaintiff and Class Members; (4) maintaining data security measures consistent with industry standards and applicable federal and state laws and other requirements; and (5) timely and adequately informing Plaintiff and Class Members if and when a data breach occurred to prevent foreseeable harm to them, notwithstanding undertaking (1)-(4) above.

91. CaptureRx had a common law duty to prevent foreseeable harm to Plaintiff and Class Members. The duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices at CaptureRx in its affirmative collection of PII and PHI from Plaintiff and Class Members. In fact, not only was it foreseeable that Plaintiff

and Class Members would be harmed by the failure to protect their PII and PHI because hackers routinely attempt to steal such information for use in nefarious purposes, CaptureRx knew that it was more likely than not Plaintiff and Class Members would be harmed as a result.

92. CaptureRx's duties to use reasonable security measures also arose as a result of the special relationship that existed between it, on the one hand, and Plaintiff and Class Members, on the other hand. This special relationship recognized in laws and regulations, arose because Plaintiff and Class Members entrusted CaptureRx with their PII and PHI by virtue of receiving health benefits through CaptureRx. CaptureRx alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

93. There is a very close connection between CaptureRx's failure to follow reasonable security standards to protect its current and former users' personal data and the injury to Plaintiff and the Class. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

94. If CaptureRx had taken reasonable security measures, data thieves would not have been able to take the personal information of Plaintiff and the Class Members. The policy of preventing future harm weighs in favor of finding a special relationship between CaptureRx and Plaintiff and the Class. If companies are not held accountable for failing to take reasonable security measures to protect the sensitive PII and PHI in their possession, they will not take the steps that are necessary to protect against future security breaches.

95. CaptureRx owed a duty to timely disclose the material fact that CaptureRx's computer systems and data security practices were inadequate to safeguard users' personal, health,

and financial data from theft.

96. CaptureRx breached these duties by the conduct alleged in the Complaint by, including without limitation, failing to protect the PII and PHI in its possession; failing to maintain adequate computer systems and data security practices to safeguard the PII and PHI in its possession; allowing unauthorized access to Plaintiff's and Class Members' PII and PHI; failing to disclose the material fact that CaptureRx's computer systems and data security practices were inadequate to safeguard the PII and PHI in its possession from theft; and failing to disclose in a timely and accurate manner to Plaintiff and members of the Class the material fact of the Data Breach.

97. But for CaptureRx's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised. Specifically, as a direct and proximate result of CaptureRx's failure to exercise reasonable care and use commercially reasonable security measures, the PII and PHI of Plaintiff and the Class Members was accessed by ill-intentioned criminals who could and will use the information to commit identity or financial fraud. Plaintiff and the Class face the imminent, certainly impending and substantially heightened risk of identity theft, fraud, and further misuse of their personal data.

98. It was foreseeable that (1) CaptureRx's failure to safeguard the PII and PHI of Plaintiff and Class Members would lead to one or more types of injury to them; and (2) data breach at CaptureRx was foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

99. As a proximate result of this conduct, Plaintiff and the other Class Members suffered damage after the unauthorized data release and will continue to suffer damages in an amount to be proven at trial. Such injuries include those described above, including one or more

of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of value of their privacy and confidentiality of the compromised PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach, reviewing bank statements, payment card, statements, insurance statements, credit reports; expenses and time spent initiating fraud alerts, decreased credit scores and ratings; lost time; lost value of PII and PHI; other economic harm; and emotional distress as a result of the Data Breach.

COUNT II
Negligence Per Se

100. Plaintiff incorporates all other allegations included in paragraph 1 through 99 of this Complaint as of fully restate herein.

101. Pursuant to the FTC Act, 15 U.S.C. § 45, CaptureRx had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiff and Class Members.

102. The FTC Act prohibits “unfair . . . practices in or affecting commerce,” which the FTC has interpreted to include businesses’ failure to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of CaptureRx’s duty in this regard. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

103. Pursuant to the Gramm-Leach-Bliley Act, CaptureRx had a duty to protect the security and confidentiality of Plaintiff’s and Class Members’ PII. *See* 15 U.S.C. § 6801.

104. Pursuant to the FCRA, CaptureRx had a duty to adopt, implement, and maintain adequate procedures to protect the security and confidentiality of Plaintiff's and Class Members' PII. *See* 15 U.S.C. § 1681(b).

105. CaptureRx solicited, gathered, and stored PII and PHI of Plaintiff and the Class Members to facilitate transactions which affect commerce.

106. CaptureRx violated the FTC Act (and similar state statutes), HIPAA, the FCRA, and the Graham-Leach-Bliley Act by failing to use reasonable measures to protect PII and PHI of Plaintiff and Class Members and not complying with applicable industry standards, as described herein. CaptureRx's conduct was particularly unreasonable given the nature and amount of PII and PHI obtained and stored and the foreseeable consequences of a data breach on CaptureRx's systems.

107. CaptureRx's violation of the FTC Act (and similar state statutes) as well as its violations of the HIPAA, the FCRA, and the Graham-Leach-Bliley Act constitutes negligence *per se*.

108. Plaintiff and the Class Members are within the class of persons that the FTC Act (and similar state statutes), HIPAA, the FCRA, and the Graham-Leach-Bliley Act were intended to protect.

109. The harm that occurred as a result of the breach is the type of harm the FTC Act (and similar state statutes), as well as the HIPAA, the FCRA, and the Graham-Leach-Bliley Act were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures caused the same harm as that suffered by Plaintiff and the Class Members.

110. As a direct and proximate result of CaptureRx's negligence *per se*, Plaintiff and Class Members have suffered, and continue to suffer, damages arising from the breach as described herein and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

111. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by CaptureRx, reviewing bank statements, payment card statements, provider and insurance statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII and PHI; and other economic and non-economic harm.

COUNT III **Declaratory Judgment**

112. Plaintiff incorporate all other allegations included in paragraph 1 through 111 of this Complaint as of fully restate herein.

113. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

114. An actual controversy has arisen in the wake of the Data Breach regarding

CaptureRx's present and prospective common law and other duties to reasonably safeguard its users' PII, and whether CaptureRx is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff and Class Members remain at imminent risk that further compromises of their PII and PHI will occur in the future. This is true even if they (or their healthcare providers) are not actively using CaptureRx's products or services.

115. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) CaptureRx continues to owe a legal duty to secure users' PII and PHI and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act;

(b) CaptureRx continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff and Class Members' PII and PHI.

116. The Court also should issue corresponding prospective injunctive relief pursuant to 28 U.S.C. §2202, requiring CaptureRx to employ adequate security practices consistent with law and industry standards to protect its users' PII and PHI.

117. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of CaptureRx. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

118. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to CaptureRx if an injunction is issued. Among other things, if another data breach

occurs at CaptureRx, Plaintiff and Class Members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to CaptureRx of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and CaptureRx has a pre-existing legal obligation to employ such measures.

119. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at CaptureRx, thus eliminating additional injuries that would result to Plaintiff, Class Members, and the millions of other CaptureRx customers whose PII and PHI would be further compromised.

RELIEF REQUESTED

Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

1. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff Rodgers as Class representative, and appoint the undersigned counsel as class counsel;
2. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and other Class Members;
3. Award restitution, compensatory, consequential, and general damages, including nominal damages as allowed by law in an amount to be determined at trial;
4. Award statutory damages to Plaintiff and Class Members in an amount to be determined at trial;
5. Award Plaintiff and Class Members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;
6. Award Plaintiff and Class Members pre- and post-judgment interest, to the extent allowable; and
7. Award such other and further relief as equity and justice may require.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demand a trial by jury of any and all issues in this action so triable as of right.

Respectfully submitted,

/s/ Jarrett L. Ellzey

Jarrett L. Ellzey

ELLZEY & ASSOCIATES, PLLC

1105 Milford Street

Houston, TX 77006

Phone: (888) 350-3931

Fax: (888) 276-3455

jarrett@ellzeylaw.com

Terence R. Coates (*pro hac vice forthcoming*)

MARKOVITS, STOCK & DEMARCO, LLC

3825 Edwards Road, Suite 650

Cincinnati, OH 45209

Phone: (513) 651-3700

Fax: (513) 665-0219

tcoates@msdlegal.com

Bryan L. Bleichner (*pro hac vice forthcoming*)

CHESTNUT CAMBRONNE PA

100 Washington Avenue South, Suite 1700

Minneapolis, MN 55401

Phone: (612) 339-7300

Fax: (612) 336-2940

bbleichner@chestnutcambronne.com